AMENDMENTS TO THE CLAIMS

Claims 1-11 (canceled)

Claim 12 (previously presented):   A method for preventing intrusions to a computer system, comprising:

using a network-based appliance to intercept data packets;

deciding whether to forward the intercepted packets or whether to route the intercepted packets to a virtual proxy;

performing TCP or UDP processing on the intercepted packets before routing them to the virtual proxy;

using the virtual proxy to analyze the packets that have been routed to the virtual proxy to detect intrusions using a processing engine having at least one processing procedure that detects intrusions; and

when the virtual proxy detects an attack or violation in the packets, using the virtual proxy to direct a transport layer to modify the packets.

Claim 13 (previously presented):   The method defined in claim 12 wherein using the virtual proxy to direct the transport layer to modify the packets further comprises:

modifying data in the packets at specified locations.

Claim 14 (previously presented)   The method defined in claim 12 further comprising using the virtual proxy to direct the transport layer to remove data from the packets when the virtual proxy detects an attack or violation.

Claim 15 (currently amended)   The method defined in claim 12, wherein the virtual proxy directs the transport layer to modify the packets using packet stream modification requests, the method further comprising sending the packet stream modification requests from the ~~an active~~ network-based appliance to a standby network-based appliance to support fault tolerance.

Claims 16-19 (canceled)